AMENDMENTS TO THE CLAIMS:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Claims 1 – 46. (Canceled)

47. (Currently Amended) A tamper-resistant electronic circuit for implementation in a device, said tamper-resistant electronic circuit comprising:

a storage device for tamper-resistantly storing, during manufacture of the tamper-resistant electronic circuit, a random secret not accessible over any external circuit interface to the tamper-resistant electronic circuit and unknown after being stored in the storage device or option;

trigger data generating circuitry for, during configuration of the tamper-resistant electronic circuit, generating trigger data using the random secret and device-specific security data that is different from the random secret and outputting the trigger data outside of the tamper-resistant electronic circuit;

a receiver for, during operation of the configured tamper-resistant electronic circuit by a user, receiving external to the tamper-resistant electronic circuit from the user via an external circuit interface the trigger data;

a cryptographic processing engine, in response to the externally received trigger data from the user, for performing cryptographic processing at least partly in response to said stored secret and the externally received trigger data from the user to generate a temporarily available instance of the device-specific security data internally confined within said electronic

circuit during usage of said device and not stored in a memory such that the temporarily available instance of the device-specific security data is only available as long as the externally received trigger data is received; and

electronic circuitry, connected to the cryptographic processing engine and configured to perform a security-related operation in response to said internally-confined, temporarily available instance of device-specific security data.

48. (Previously Presented) The electronic circuit according to claim 47, wherein said device is a network device and said operation is related to at least one of data confidentiality, data integrity, authentication, authorization and non-repudiation in network communication.

49. (Previously Presented) The electronic circuit according to claim 47, wherein said device is configured for producing digital content and said security-related operation is configured for marking said digital content based on said internally-confined, temporarily available instance of device-specific security data.

50. (Previously Presented) The electronic circuit according to claim 49, wherein said operation is configured for generating a device-specific fingerprint embedded into said digital content.

51. Canceled.

52. (Previously Presented) The electronic circuit according to claim 47, said electronic circuit comprises:

means for generating, based on said stored secret and said configurational device-specific security data, said trigger data as a cryptographic representation of said configurational device-specific security data during configuration of said device;

means for outputting said cryptographic representation over an external circuit interface during configuration; and

means for internally re-generating said device-specific security data during usage of said device provided that said additional input corresponds to said cryptographic representation.

53. Canceled.

54. (Previously Presented) The electronic circuit according to claim 52, wherein said means for internally re-generating said device-specific security data comprises means for generating a private key at least partly based on said stored secret, and said trigger data is generated as a cryptographic representation of said private key during configuration of said device.

55. (Previously Presented) The electronic circuit according to claim 47, further comprising means for making, during configuration of said device, said internally-confined, temporarily available instance of device-specific security data available over the external circuit interface provided that a predetermined device access code is entered into the electronic circuit.

56. (Previously Presented) The electronic circuit according to claim 47, further comprising means for disabling internal access to at least one of said stored secret and said device-specific security data unless a predetermined device access code is entered into the electronic circuit.

57. (Previously Presented) The electronic circuit according to claim 55, further comprising:

means for authentication of a manufacturer of said device;

means for providing, during device manufacturing, said device access code to said device manufacturer in response to successful authentication.

58. (Previously Presented) The electronic circuit according to claim 47, wherein said electronic circuitry comprises:

means for performing additional cryptographic processing based on said internally-confined, temporarily available instance of the device-specific security data and further external input data to generate further security data; and

means for performing said security-related operation in response to said further security data.

59. (Previously Presented) The electronic circuit according to claim 58, wherein said device-specific security data represents a private key, and said further external input data

represents an encryption of said further device-specific security data by the corresponding public key.

60. (Previously Presented) The electronic circuit according to claim 59, wherein said further security data represents a symmetric content decryption key issued by a content provider, and said device-specific security data represents a private key of a device manufacturer.

61. (Previously Presented) The electronic circuit according to claim 47, wherein said cryptographic processing engine is configured for generating a symmetric cryptographic key in response to a seed applied over an external circuit interface.

62. (Previously Presented) The electronic circuit according to claim 47, wherein said cryptographic processing engine is configured for generating an internally-confined, temporarily available private key at least partly based on said stored secret, and said electronic circuitry comprises means for performing asymmetric cryptography operations based on said internally confined, temporarily available private key.

63. (Previously Presented) The electronic circuit according to claim 62, further comprising means for generating a public key corresponding to said private key during configuration of said device, and means for outputting said public key over an external circuit interface.

64. (Previously Presented) The electronic circuit according to claim 62, further comprising:

means for performing shared key generation to generate a new shared key based on said generated private key and a public key of an intended communication partner; and

means for performing cryptographic processing based on said new shared key.

65. (Previously Presented) The electronic circuit according to claim 47, wherein said cryptographic processing engine is configured for generating said internally-confined, temporarily available instance of device-specific security data as a chain of *k* bind keys $B_1, \ldots, B_k$ in response to corresponding bind identities $R_1, \ldots, R_k$ according to the following formula:

$$B_i = f(B_{i-1}, R_i) \qquad \text{for } i=1, \ldots, k,$$

where B_0 represents the stored secret, and f is a cryptographic one-way function.

66. (Currently Amended) A device implemented with a tamper-resistant electronic circuit, said electronic circuit comprising:

a storage unit for tamper-resistantly storing, during manufacture of the tamper-resistant electronic circuit, a random secret not accessible over any external circuit interface to the tamper-resistant electronic circuit and unknown after being stored in the storage device or option;

trigger data generating circuitry for, during configuration of the tamper-resistant electronic circuit, generating trigger data using the random secret and device-specific security

data that is different from the random secret and outputting the trigger data outside of the tamper-resistant electronic circuit;

a receiver for, during operation of the configured tamper-resistant electronic circuit by a user, receiving external to the tamper-resistant electronic circuit from the user via an external circuit interface the trigger data;

a cryptographic processing engine, in response to the externally received trigger data from the user, for performing cryptographic processing at least partly in response to said stored secret and the externally received trigger data from the user to generate a temporarily available instance of the device-specific security data internally confined within said electronic circuit during usage of said device and not stored in a memory such that the temporarily available instance of the device-specific security data is only available as long as the externally received trigger data is received; and

electronic circuitry, connected to the cryptographic processing engine and configured to perform a security-related operation in response to said internally-confined, temporarily available instance of device-specific security data.

67. (Previously Presented) The device according to claim 66, wherein said device is a network device and said operation is related to at least one of data confidentiality, data integrity, authentication, authorization and non-repudiation in network communication.

68. (Previously Presented) The device according to claim 66, wherein said device is configured for producing digital content and said security-related operation is configured for marking said digital content based on said device-specific security data.

69. (Previously Presented) The device according to claim 66, wherein said cryptographic processing engine is configured for generating said internally-confined, temporarily available instance of device-specific security data provided that additional input data in the form of predetermined trigger data is applied over an external circuit interface of the electronic circuit during usage of said device, wherein said trigger data is defined during configuration of said device.

70. (Currently Amended) A method for a device, said method comprising the steps of:

storing, in a controlled environment during manufacturing of a tamper-resistant electronic circuit, a secret randomized number in said electronic circuit such that the secret randomized number is not available outside of said tamper-resistant electronic circuit and is unknown after being stored in the storage device or option;

during configuration of the tamper-resistant electronic circuit, generating trigger data using the secret randomized number and device-specific security data that is different from the secret randomized number and outputting the trigger data outside of the tamper-resistant electronic circuit;

implementing, during circuit manufacturing, functionality into said electronic circuit for, during operation of the configured tamper-resistant electronic circuit by a user, receiving external to the tamper-resistant electronic circuit from the user via an external circuit interface the trigger data;

implementing, during circuit manufacturing, functionality into said electronic circuit for, in response to the externally-received trigger data from the user, performing cryptographic processing at least partly based on said stored secret number and the externally-received trigger data from the user to generate a temporarily available instance of the device-specific security data internally confined within said electronic circuit during usage of the device and not stored in a memory such that the temporarily available instance of the device-specific security data is only available as long as the externally received trigger data is received;

implementing, during circuit manufacturing, a security-related operation into said electronic circuit, said security-related operation being configured for receiving at least said internally-confined, temporarily available instance of device-specific security data as input during usage of the device; and

installing, during device manufacturing, said electronic circuit into said device.

71. (Previously Presented) The method according to claim 70, wherein said device is a network device and said operation is related to at least one of data confidentiality, data integrity, authentication, authorization and non-repudiation in network communication.

72. (Previously Presented) The method according to claim 70, wherein said device is configured for producing digital content and said security-related operation is configured for marking said digital content based on said internally-confined temporarily available instance of device-specific security data.

73. (Previously Presented) The method according to claim 70, further comprising the step of providing, during configuration of the device, trigger data to be applied later during usage of the device in order to be able to generate said internally-confined temporarily available instance of device-specific security data within said electronic circuit.

74. (Currently Amended) The method according to claim 73, further comprising the steps of:

entering, in a controlled environment during device configuration, said trigger data as input data into said electronic circuit in order to obtain device-specific security data from the cryptographic functionality of the electronic circuit;

recording, in a controlled environment during device configuration, said device-specific security data and said input data; and

entering, in a controlled environment during device configuration, a predetermined device access code into the electronic circuit for accessing the internally-confined temporarily available instance of device-specific security data over an external circuit interface.

75. (Currently Amended) The method according to claim 73, further comprising the steps of:

generating, in a controlled environment during device configuration, an internally-confined temporarily available instance of device-specific security data;

entering, in a controlled environment during device configuration, said generated device-specific security data into said electronic circuit in order to obtain said trigger data as a result representation from the cryptographic functionality of the electronic circuit; and

recording, in a controlled environment during device configuration, said result representation and the previously generated device-specific security data.